UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/718,786	11/21/2003	Charles Douglas Ball	RPS920030189US1	1539

55128 7590 07/13/2007

LENOVO - JVL
C/O VANLEEUWEN & VANLEEUWEN
P.O. BOX 90609
AUSTIN, TX 78709-0609

EXAMINER	
SHAN, APRIL YING	
ART UNIT	**PAPER NUMBER**
2135	
MAIL DATE	**DELIVERY MODE**
07/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/718,786	**Applicant(s)** BALL ET AL.	
	Examiner April Y. Shan	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 26 April 2007.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1,3-21 and 23-30 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1, 3-21 and 23-30 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

1. The Applicant's amendment, filed 26 April 2007, has been received, entered into the record, and respectfully and fully considered.

2. As a result of the amendment, claims 1, 3, 11, 13, 21, 23, 24 and 26 have been amended. Claims 2, 12 and 22 have been canceled. Claims 1, 3-11, 13-21 and 23-30 are now presented for examination.

3. Any objections/rejections not repeated below for record are withdrawn due to Applicant's amendment.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 21 and 23-30 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Regarding **claims 21 and 23-30**, the Applicant's efforts to overcoming the rejection is acknowledged. Now, the computer program product stored on a computer operable medium. However, the rest of newly added claim limitation "...for execution by a computer, which, when executed by the computer, cause the computer to implement a method..." is still non-statutory. It appears to the examiner that "for execution" is the intended use and "which, when executed by the computer, cause..." is optional, which means the method is not always implemented.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

8. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

9. Claims 1, 3-11, 13-21 and 23-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kern et al. (U.S. Patent No. 6,336,187) in view of Kohara et al. (U.S. Pub. No. 2003/0182566)

As per **claims 1 and 11**, Kem et al. discloses a method/apparatus comprising:

Encrypting ("encoding" – e.g. col. 10, line 12 and "public key encryption" – e.g. col. 10, line 30) a plurality of non-volatile storage regions ("..The storage 108 may be implemented by one or more storage devices of various types, such as magnetic disk drive, magnetic tape, optical disk..." – e.g. col. 5, line 60 – col. 6, line 4 and "The nonvolatile storage 206 may comprise, for example, one or more magnetic data storage disks such as a "hard drive", a tape drive, or any other suitable storage device" – e.g. col. 6, lines 23-25), each being encrypted using a different ("...initially storing a security key in association with a storage region..." – e.g. abstract and col. 1, lines 46-49) encryption key ("As an enhancement to the embodiment described above, the controller 106 may direct the storage 108 to employ the reference access key in encoding or decoding data during the storage operation of step 516. In this embodiment, if the requested storage area is protected (i.e., it has an associated reference access key), and the host-submitted input access key is valid, the controller 106 uses the access key to encode or decode data involved in the storage access operation...Encoding and decoding in this embodiment may use a number of different techniques that are well known to those in the relevant art. For instance, one useful technique is public key encryption. By using such encoding/decoding, stored data enjoys two levels of protection....by encoding data of the storage region with the key" – e.g. col. 10, lines 10-35);

granting the first user ("one or more hosts" – e.g. abstract. Please note one or more hosts corresponds to Applicant's first user and second user) access to a corresponding first subset of non-volatile storage regions (e.g. col. 2, line 64 - col. 3, line 9) and making a second subset of the encryption keys available to a second user thereby granting the second user ("one or more hosts" – e.g. abstract. Please note one or more hosts corresponds to Applicant's first user and second user.) access to a corresponding second subset of non-volatile storage regions (e.g. col. 2, line 64 - col. 3, line 9).

generating a first private-public encryption key pair and a second private-public encryption key pair ("public key encryption" – e.g. col. 10, line 30. Please note to a person with ordinary skill in the art that public key encryption is an asymmetric algorithm are designed so that the key used for encryption is different from the key used for decryption. Therefore, it must generate a key pair for the first user and the second user);

making the first private key available only to the first user and the second private key only to the second user (e.g. col. 7, lines 49-59); and

encrypting the first subset of the encryption keys using the first public encryption key, and the second subset of the encryption keys using the second public encryption key (e.g. col. 10, lines 27-35, col. 5, lines 47-48 and col. 10, lines 10-20 and please see below response to the argument item 11).

Kern et al. does not disclose expressly the encryption key is from a set of encryption keys, making a first subset/second subset of the encryption keys available to the first user/second user thereby granting the first user/second user, the first/second subset of the encryption keys consisting of one, a plurality, or all of the encryption keys.

Kohara et al. discloses the encryption key is from a set of encryption keys, making a first subset/second subset of the encryption keys available to the first user/second user and the first/second subset of the encryption keys consisting of one, a plurality, or all of the encryption keys (e.g. paragraphs [0010] - [0012], par. [0052] and abstract. Please also see below response to argument item 12)

Kern et al. and Kohara et al. are analogous art because they are from the same field of endeavor of protecting data stored on nonvolatile storage section.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to incorporate the encryption key is from a set of encryption keys, making a first subset/second subset of the encryption keys available to the first user/second user into Kern et al.'s method/apparatus.

The motivation of doing so would have been "generated plural encryption keys make a very low probability of occurrence of an identical encryption key because the pseudorandom number is used for the encryption key c. Consequently, allocation of the generated latest encryption key to the user can differ the plural encryption keys allocated at the different generation timings of the pseudorandom numbers at a high probability. This allows data encryption keys, and it is possible to store plural kinds of encrypted data, each of which has a different encryption key, in the nonvolatile storage section" and "to prevent the non-interested persons from recognizing stored data in a nonvolatile storage medium in chain manner", as taught by Kohara et al. (paragraphs [0007] and [0012])

As per **claims 3 and 13**, the combined teachings of Kern et al. and Kohara et al. discloses a method/apparatus as applied above in claims 2 and 12. Kern et al. further discloses comprising:

storing the first private key and the second private key in a secure memory unit (Kern et al. – e.g. col. 5, lines 33-48);

protecting access to the first private key with a first authentication token, the first authentication token being known only to the first user (e.g. col. 9, line 63 – col. 10, line 9); and

protecting access to the second private key with a second authentication token, the second authentication token being known only to the second user (e.g. col. 9, line 63 – col. 10, line 9).

As per **claims 4 and 14**, the combined teachings of Kern et al. and Kohara et al. discloses a method/apparatus as applied above in claims 3 and 13. Kern et al. further discloses comprising:

requesting an authentication token from a user attempting to access one or more of the non-volatile storage regions (e.g. col. 2, line 64 – col. 3, line 9);

authenticating the user, if the user's authentication token matches
one of the authentication tokens used to protect access to one of the private
keys (e.g. col. 2, line 64 – col. 3, line 9);

decrypting, with the secure encryption module using the authenticated user's private key, a corresponding subset of encryption keys, in response to authenticating the user (e.g. col. 10, lines 10-35); and

decrypting a corresponding subset of non-volatile storage regions, thereby making the corresponding subset of non-volatile storage regions available to the authenticated user (e.g. col. 10, lines 10-35).

As per **claims 5 and 15**, the combined teachings of Kern et al. and Kohara et al. discloses a method/apparatus as applied above in claims 3 and 13. Kern et al. further discloses wherein the authentication tokens are selected from the group consisting of: passwords, fingerprints signatures, voice signatures, retina signatures, and secure access devices (e.g. col. 7, lines 49-62).

As per **claims 6 and 16**, the combined teachings of Kern et al. and Kohara et al. discloses a method/apparatus as applied above in claims 4 and 14. Kohara et al. further discloses wherein the encrypting and decrypting the plurality of non-volatile storage regions are performed using full-disk encryption software ("In an encryption storage apparatus..." – e.g. abstract).

As per **claims 7 and 17**, the combined teachings of Kern et al. and Kohara et al. discloses a method/apparatus as applied above in claims 1 and 11. Kern et al. further discloses wherein one of the non-volatile storage regions is adapted to store an operating system and data common to the first user and to the second user (e.g. col. 1, lines 45-50 and col. 1, lines 59-65).

As per **claims 8 and 18**, the combined teachings of Kern et al. and Kohara et al. discloses a method/apparatus as applied above in claims 1 and 11. Kern et al. further discloses wherein one of the non-volatile storage regions is adapted to store user-specific data of the first user (e.g. col. 1, lines 45-46 and lines 49-50).

As per **claims 9 and 19**, the combined teachings of Kern et al. and Kohara et al. discloses a method/apparatus as applied above in claims 1 and 11. Kern et al. further discloses wherein one of the non-volatile storage regions is adapted to store user-specific data of the second user (e.g. col. 1, lines 45-46 and lines 49-50).

As per **claims 10 and 20**, the combined teachings of Kern et al. and Kohara et al. discloses a method/apparatus as applied above in claims 1 and 11. Kern et al. further discloses wherein the non-volatile storage regions are chosen from the group consisting of: volumes, disks, partitions, and folders/directories ("..The storage 108 may be implemented by one or more storage devices of various types, such as magnetic disk drive, magnetic tape, optical disk…" – e.g. col. 5, line 60 – col. 6, line 4 and "The nonvolatile storage 206 may comprise, for example, one or more magnetic data storage disks such as a "hard drive", a tape drive, or any other suitable storage device" – e.g. col. 6, lines 23-25).

As per **claims 21 and 23-30**, the combined teachings of Kern et al. and Kohara et al. discloses the claimed method of steps as applied above in claims 1-10. Therefore, the combined teachings of Kern et al. and Kohara et al. disclose the claimed computer program product for carrying out the method of steps.

Response to Arguments

10. Applicant's arguments filed 26 April 2007 have been respectfully and fully considered but they are not persuasive.

11. The Applicant's essential argument is "Kern is only encrypting the data in the storage region. Kern does not teach or suggest encrypting an access key which is then used to further encrypt the data in the storage region" (see page 14 of the remark) and "neither Kern or Korhara teaches or suggests encrypting the encryption key in the manner taught and claimed by Applicants" (see page 13 of the remark), the examiner respectfully disagrees.

First, the examiner respectfully points out in col. 5, lines 47-48, Kern et al. discloses "Furthermore, Table 1 may be **encrypted** by controller 106 **to secure the access key from accidental/malicious access**" (Please note access key is part of table 1.) and in col. 10, lines 10-20, Kern et al. further discloses "...the controller 106 may direct the storage 108 to **employ the reference access key in encoding or decoding data** during the storage operation of step 516...the controller 106 uses the access key to encode or decode data involved in the storage access operation...". Kern et al. further teaches "Encoding and decoding data..may use a number of different techniques that are well known to those in the relevant art. For instance, one useful technique is **public key encryption**."

Second, the examiner respectfully points out in par. [0037] of the Kohara et al. reference, Kohara et al. discloses "...Fig. 2(b), which is the addition of an encryption key randomization section 9 for generating a pseudorandom number e, by making the encryption key c as a trigger, and for inputting the pseudorandom number e to the EX-OR gate 8...to generate the encrypted data d2...In the arrangement in Fig. 2(b), even a simple sequence of numeric value is randomized into a complex sequence of numeric values so that the encryption key c cannot be easily guessed by the analysis of the encrypted data d2.

Third, the examiner respectfully points out although the Applicant argues on page 10 of the remark, "...that each users' encryption keys are encrypted with an encryption key that is specific to the corresponding user", this claim limitation is **not** recited in the claim. Instead, the claims 1, 11 and 21 only recite "making the first **private** key available only to the first user and the second **private** key available only to the second user...**encrypting** the first subset of the encryption keys using the first **public** encryption key, and the second subset of the encryption keys using the second **public** encryption key", therefore, only the first **private** key and the second **private** key are specific to the corresponding user, **not** the first **public** key and the second **public** key. The Applicant is respectfully reminded that although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns, 988 F. 2d 1181, 26 USPQ 2d 1057 (Fed. Cir. 1993).*

Fourth, the examiner respectfully request the Applicant, in preparing the response, to consider fully the entire refernce as potentially teaching all or part of the claimed invention, as well as the context of the passages as taught by the prior art or disclosed by the examiner.

12. Applicant argues "Kohara does not teach or suggest making a first subset...and making a second subset of the encryption keys available to a second user", the examiner respectfully disagrees.

Kohara discloses in par. [0012] "...Consequally, allocation of the generated latest encryption key to the user can differ the plural encryption keys allocated at the different generation timings of the pseudorandom numbers at a high probability" and in par. [0052], Kohara further discloses "...plural encryption keys c are stored...Therefore, the encryption keys c can be used for the encryption and decryption of different kinds of data, respectviely, so that it is possible to allocate different encryption keys c to different users in the same period and to allocate to the same user mutually different encryption keys c for the processing of the different kinds of data...thereby improving the efficiency in data encryption and decryption".

13. Regarding Applicant's argument on page 15 towards the dependent claims 3-4, 13-14 and 23-24 being allowable due to dependency. However, because the arguments for the independent claims are traversed, the dependent claims are also not allowable.

Conclusion

14. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYS
25 June 2007
AYS

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100